ISA 201
Intermediate Information Systems Acquisition

Lesson 10
Risk Management

Learning Objectives

Today we will learn to:

- Define the elements that constitute an effective Risk Management (RM) program for an Information Technology (IT) system acquisition.
- Identify the two components of risk.
- Identify how risk, issue, and opportunity management interrelate.
- Identify risks inherent to IT system acquisition.
- Apply the five components of the DOD Risk Management Process Model to a given IT acquisition scenario.

Lesson Plan

- Risk Overview
- Risk, Issue, and Opportunity Relationship
- IT Related Risks
- Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
- Lesson Review

“If you don’t actively attack the risks, they will actively attack you.” Tom Gilb
Principles of Software Engineering Management

Guidance & Policy

USD/AT&L Perspective

Our task as managers involves optimization—what are the highest-payoff risk-mitigation investments we can make with the resources available?

From the Under Secretary of Defense for Acquisition, Technology, and Logistics
Risk and Risk Mitigation—
Don't Be a Spectator
Frank Kendall

Defense AT&L: January - February 2015

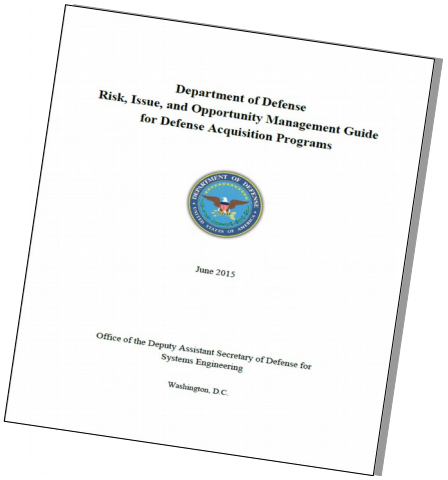
DODI 5000.02 7Jan15

Chap 6. PROGRAM MANAGEMENT RESPONSIBILITIES.

The Program Manager is responsible for implementing effective risk management and tracking to include the identification of all known risks, key assumptions, probability of occurrence, consequences of occurrence (in terms of cost, schedule, and performance) if not mitigated, analysis of mitigation options, decisions about actions to mitigate risk, and execution of those actions

DoD Risk, Issue, and Opportunity Guide, June 2015

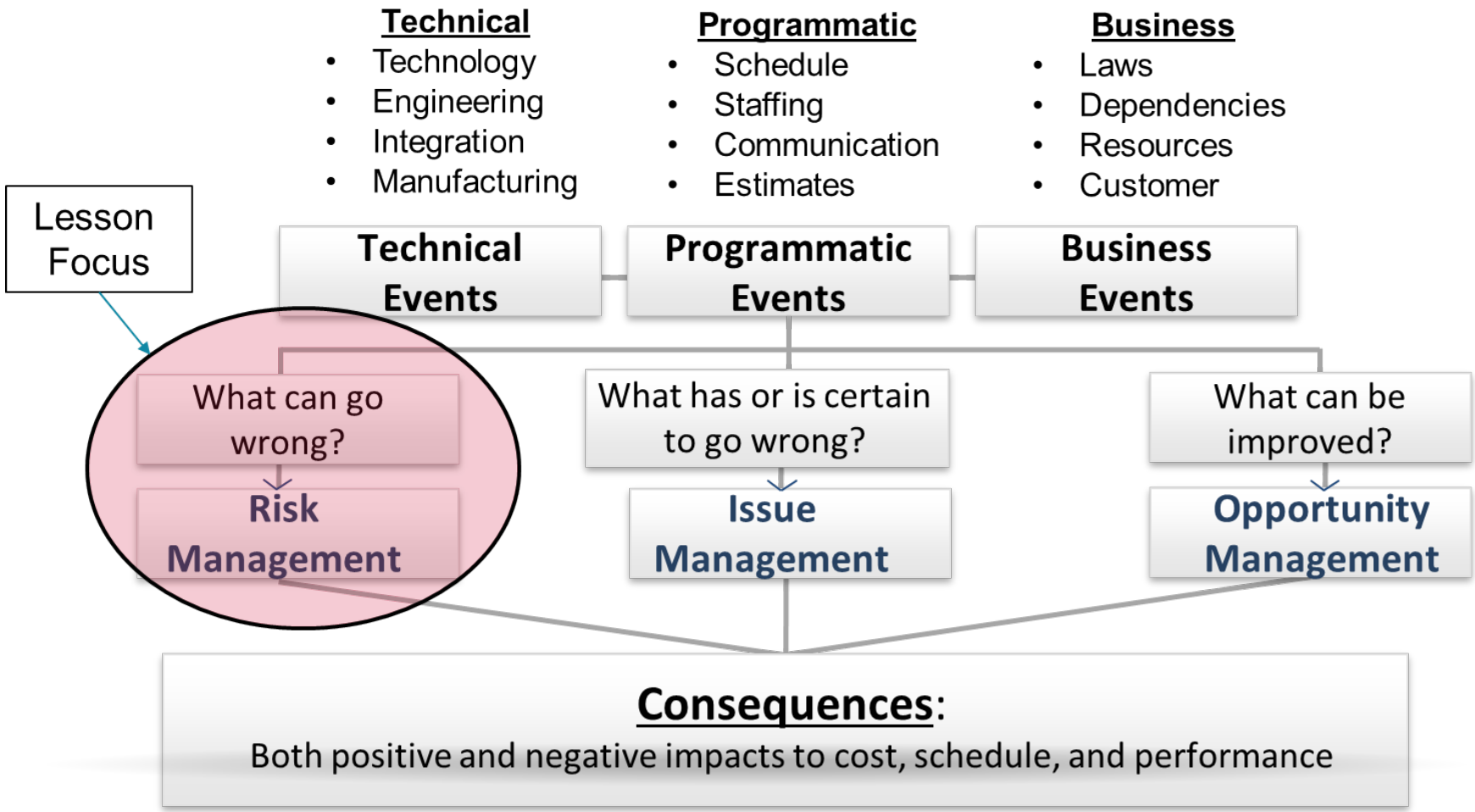
- Markedly different from DoD Risk Management Guide (RMG), Version 6.0, August, 2006
- Title changed to: DoD Risk, Issue, and Opportunity Management Guide (RIOMG) for Defense Acquisition Programs - June 2015


Department of Defense
Risk, Issue, and Opportunity Management Guide
for Defense Acquisition Programs
June 2015
Office of the Deputy Assistant Secretary of Defense for
Systems Engineering
Washington, D.C.

DoD RIOM Guide Content

- Section 1: Introduces the scope and changes
- Section 2: Describes planning & documentation of program's risk management process.
- Section 3: 5-step risk management process: planning, identification, analysis, handling, and monitoring.
- Section 4: Integrating risk management with other program management tools.
- Section 5: Issue Management - differentiates between Risk and Issue Management.
- Section 6: Opportunity Management.
- Section 7: Internal and external interfaces with interdependent programs and cross-program risks.

Risk, Issue, and Opportunity Relationship



Risk Definition

Risk is the combination of:

1. the probability of an undesired event
   or condition and
2. the consequences, impact, or severity
   of the undesired event, were it to occur.*

The undesired event may be programmatic
or technical, and either internal or external
to the program.

* DOE Risk, Issue, and Opportunity Management Guide June 2015

Risks and Issues

Issues: Current Problems: Focus is on Real-Time Consequences

Risks: Future Problems: Focus is on Future Consequences and Likelihood

RISK or ISSUE?

If it has already occurred, it's an Issue, not a Risk

Issues may create additional potential Risks

Lesson Plan Status

- Risk Overview
- Risk, Issue, and Opportunity Relationship
- IT Related Risks
- Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
- Lesson Review

"If you don't actively attack the risks, they will actively attack you." Tom Gilb
Principles of Software Engineering Management

Issue Management

- Applies resources to address and resolve the consequences associated with a past, present, or certain future event.
- Programs also should assess whether issues may create **additional potential risks**, and evaluate them accordingly.
- Issue management and opportunity management are complementary to the risk management process.

Issue Monitoring
How has the issue changed?
Issue Planning
What is the program's issue management process?
Issue Identification
What has or will go wrong?
Issue Analysis
What is the consequence of the issue?
Issue Handling
Should the issue be accepted, avoided, transferred, or mitigated?
Communication and Feedback

The key is to ensure proper focus on both issues and risks so that attention on current problems will not overtake efforts to manage risks and opportunities

Issue Management Analysis

- Approved issues should be analyzed using the **program's risk management consequence criteria**, and the results entered into an issue tracking register.
- Unlike opportunities and risks, **no evaluation of issue likelihood is necessary** as the probability=1.
- Using the top row from the risk matrix, the issue consequence value is then converted to an issue level using the **issue reporting matrix.**
- The results are entered into the program's issue tracking register.

Issue reporting matrix

Issue	Consequence	Type T/B/P	Plan of Action and Milestones			
			Closure Activities	Closure Date Planned (P) Actual (A)	Cost	
					Type (RDT&E, Procurement, O&M)	Amount ($)
Issue X (Describe the issue that has occurred or will occur, the type of issue [technical, business, or programmatic], and the resulting cost, schedule, and performance consequences)		Tech (T)	Activity 1	(P) – 10/12/13 (A) - 11/1/13	RDT&E	$420K
			Activity 2	(P) (A)	Procurement	$2.1M
			Activity 3	(P) (A)		
				(P) (A)		
				(P) (A)		
				(P) (A)		
				(P) (A)		
				(P) (A)		
				(P) (A)		

Issue Tracking Register

DoD Risk, Issue, and Opportunity Management Guide June 2015

Issue Management Expectations

- Programs should not confuse issues with risks.
- Issues are assessed for residual risks and formal risks are established as appropriate.
- Programs document an issue management process.
- The process may share elements with the risk management process, while respecting differences.
- Programs develop a plan to address, track, and review issues during regular meetings and reviews.
- Programs track cost, schedule, and performance issues and report to the appropriate management

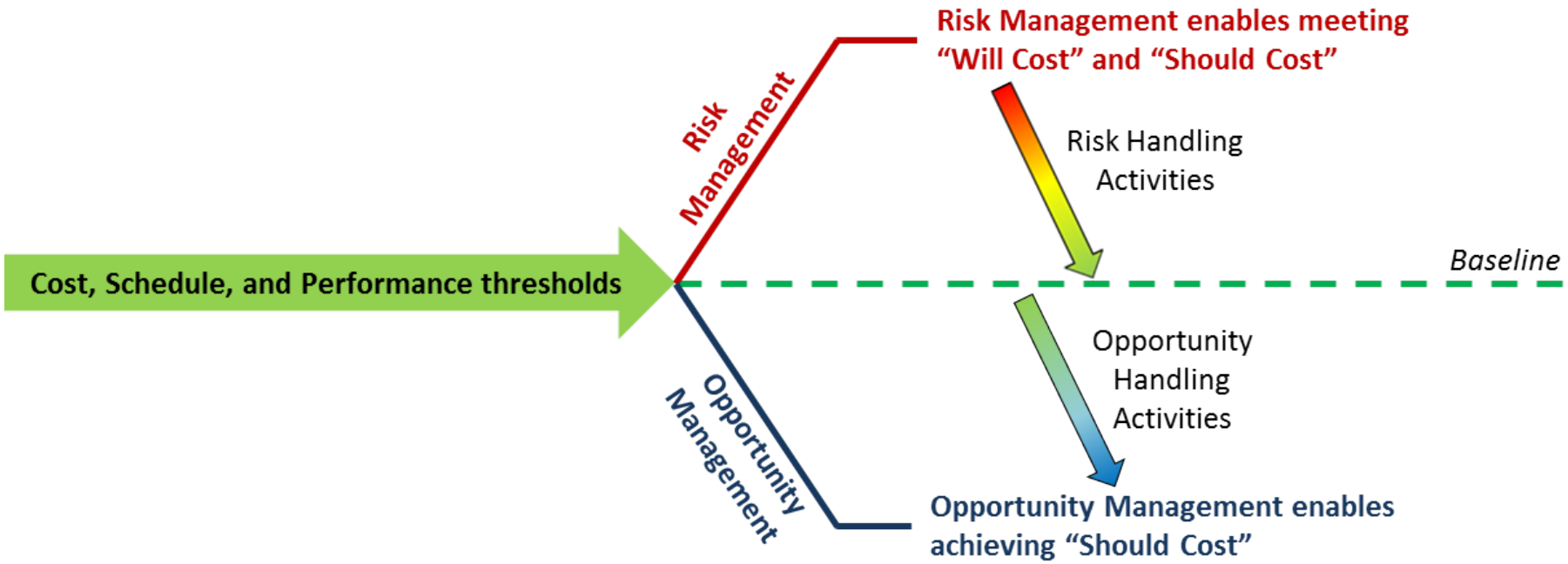
Opportunity Management

- Opportunities are potential future benefits to the program's cost, schedule, and/or performance baseline.
- The program identifies potential enhancements to cost, schedule, and/or performance.
- Measures potential program improvement in terms of likelihood and benefits.
- Opportunities should be evaluated for both advantages and disadvantages.

Opportunity Monitoring
How has the opportunity changed?
Opportunity Planning
What is the program's opportunity management process?
Communication and Feedback
Opportunity Identification
What can be improved?
Opportunity Analysis
What is the business case analysis of the opportunity?
Opportunity Handling
Should the opportunity be pursued, reevaluated, or rejected?

Opportunity management, like issue management, should be considered as complementary to risk management.

Opportunity Management Expectations



- PMs use opportunity management to plan, identify, analyze, handle, and monitor initiatives that potentially yield improvements in the cost, schedule, and/or performance baseline.
- Programs evaluate approved opportunities and manage any associated risks.

Programs establish opportunity likelihood and benefit criteria in line with program "should-cost" objectives.

Better Buying Power

- **Achieve Affordable Programs**
- **Control Costs Throughout the Product Lifecycle**
- **Incentivize Productivity & Innovation in Industry and Government**
- **Eliminate Unproductive Processes and Bureaucracy**
- **Promote Effective Competition**
- **Improve Tradecraft in Acquisition of Services**
- **Improve the Professionalism of the Total Acquisition Workforce**

Should Cost Management

- All acquisition managers should **routinely analyze all cost elements** and look at reasonable measures to reduce them with prudent consideration of risks
- Don’t accept the Independent **Cost Estimate** (ICE) as a self-fulfilling prophesy
- The goal is **not** to spend the budget—it’s to get all the value for the budget
- Should cost targets are required for all Acquisition Category (ACAT) I–III (services and products) programs

Note: Should Cost is for internal DoD use, not for budget planning

Lesson Plan Status

- Risk Overview
- Risk, Issue, and Opportunity Relationship
- **IT Related Risks**
- Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
- Lesson Review

Sources/Categories of Common IT Risks

- Changing and/or creeping requirements
- Software development
- Pace of tech advancement
- Mature technology availability challenges
- Technical feasibility
- Interdependence of parallel projects
- Sheer # and scope of projects
- Funding availability & stability
- Commercial Off the Shelf (COTS)
- System integration
- Software Reuse
- Architecture challenges
- Cybersecurity
- Data quality challenges
- Interfaces (user, data, communications, …)
- Personnel/ Training challenges

Lesson Plan Status

- Risk Overview
- Risk, Issue, and Opportunity Relationship
- IT Related Risks
- Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
- Lesson Review

Risk Management

- Risk management is an integral part of program management and systems engineering.
- Successful risk management requires thoughtful planning and resourcing, and should be implemented as early as possible in the life cycle.
- Effective qualitative and quantitative risk, issue, and opportunity management are critical to a program's success.

Risk Monitoring
How has the risk changed?
Risk Planning
What is the program's risk management process?
Communication and Feedback
Risk Handling
Should the risk be accepted, avoided, transferred, or mitigated?
Risk Identification
What can go wrong?
Risk Analysis
What are the likelihood and consequence of the risk?

The goal is to identify risks and handling strategies to inform decisions before they become issues

Risk Management Approach

It is essential that programs define, implement, and document an appropriate risk management approach that is organized, comprehensive, and iterative by addressing the following questions:

- Risk Planning: What is the program's risk management process?
- Risk Identification: What can go wrong?
- Risk Analysis: What is the likelihood and consequence of the risk?
- Risk Handling (**Mitigation**): Should the risk be accepted, avoided, transferred, or mitigated?
- Risk Monitoring (**Tracking**): How has the risk changed?

Sound Risk Management

- Helps identify and anticipate problems
- Provides for sufficient response time
- Eliminates many surprises
- Provides pro-active approach
- Prevents loss of: revenue, time and mission success

One risk-mitigation rule of thumb for program planning is to do the hard things first.

Hon. Frank Kendall, USD/AT&L

Risk Management Obstacles

- **Culture** often precludes risk management
  - I know what I'm doing
- **Going through the motions** vs. an Integral process
  - Time for another quarterly brief
- Management and organizations fear risk identification
  - It's not my fault
  - If I don't know, then no one can blame me
- **Issues vs. risks**—they are not the same
  - I just lost $2M in the budget review
- Process is **not supported by infrastructure**
  - Who is in charge of risk management?

Risk Planning

Risk planning consists of the activities to develop, implement, and document the risk management process. Effective planning should outline each of the risk management steps

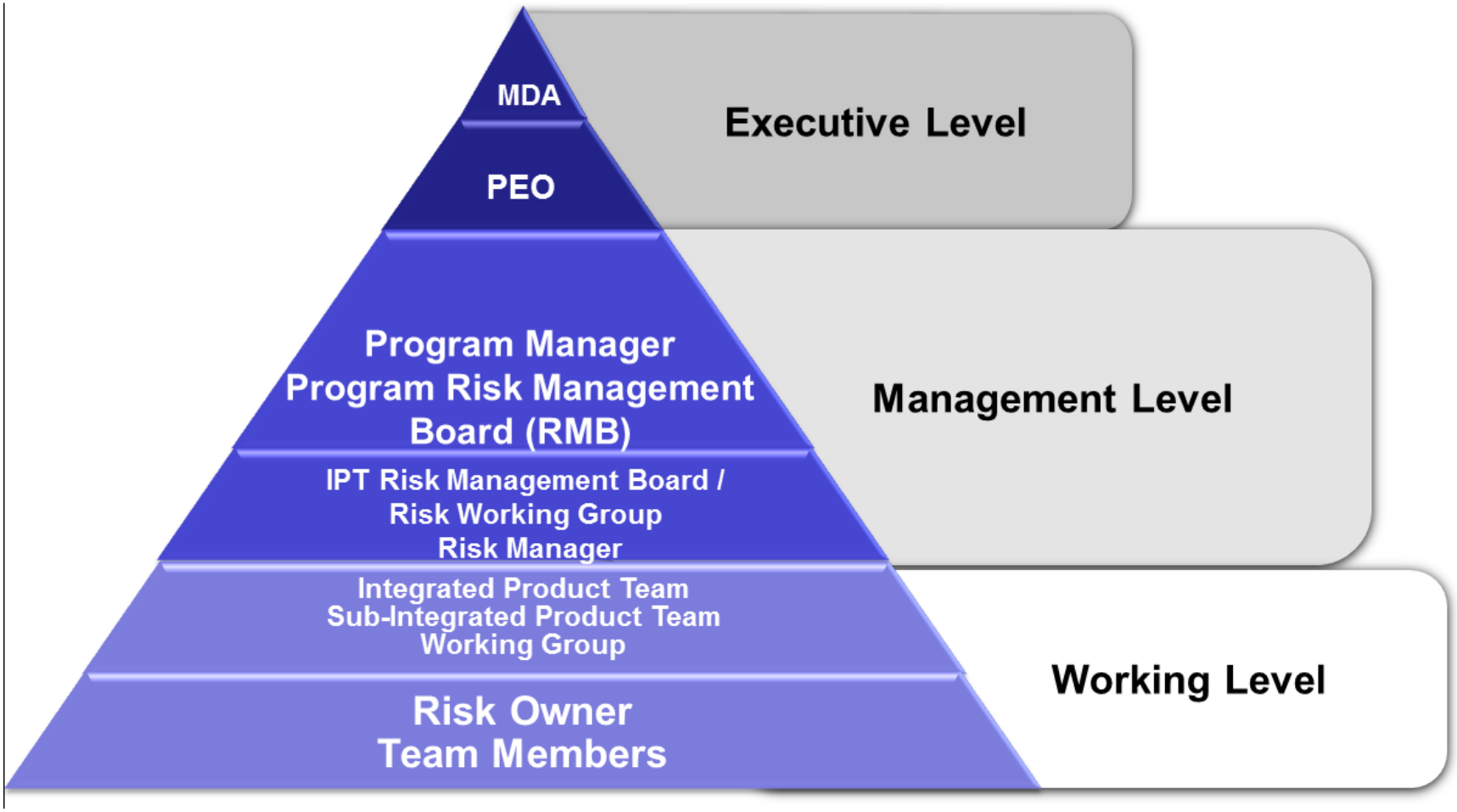
Risk Planning
What is the program's risk management process?
Risk Identification
What can go wrong?
Risk Analysis
What are the likelihood and consequence of the risk?
Risk Handling
Should the risk be accepted, avoided, transferred, or mitigated?
Risk Monitoring
How has the risk changed?
Communication and Feedback

Risk planning should be summarized in the System Engineering Plan (SEP) and the Risk Management Plan (RMP) and should address:

- the program's risk management organization
- ground rules and assumptions
- candidate risk categories
- use of any risk management tools.

"Everyone has a plan, 'till they get punched in the mouth" Mike Tyson

Roles/Responsibilities



Details of Roles and Responsibilities contained in Appendix D of RIOMG

Risk Management Plan (RMP)

- DoD programs are required to summarize the risk management approach and planning activities in the SEP and Acquisition Strategy.
- Some programs document their plans in a combined Risk, Issue, and Opportunity (RIO) Management Plan or in a Risk Management Plan (RMP).

Suggested RMP outline:

- Introduction
- Program Summary
- Definitions
- Risk Management Strategy
- Risk Management Board(s) and Risk Working Group(s)
- Roles, Responsibilities, and Authorities
- Risk Management Process and Procedures
- Risk Management in Relation to Other PM Tools
- Risk Evaluation Techniques
- Communicating and Feedback Process

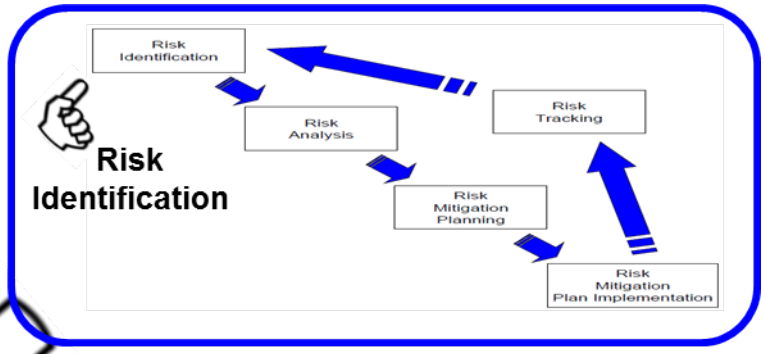
Identifying Risk: What Can Go Wrong?

“I cannot imagine any conditions which would cause a ship to founder. I cannot conceive of any vital disaster happening to this vessel. Modern shipbuilding has gone beyond that ..."

Captain E.J. Smith, 1906, about the Adriatic

(Captain of Titanic on the evening on 14 April, 1912)

Risk Identification in DoD RMG v6 and DoD RIOMG Models



DoD RMG v6 August, 2006

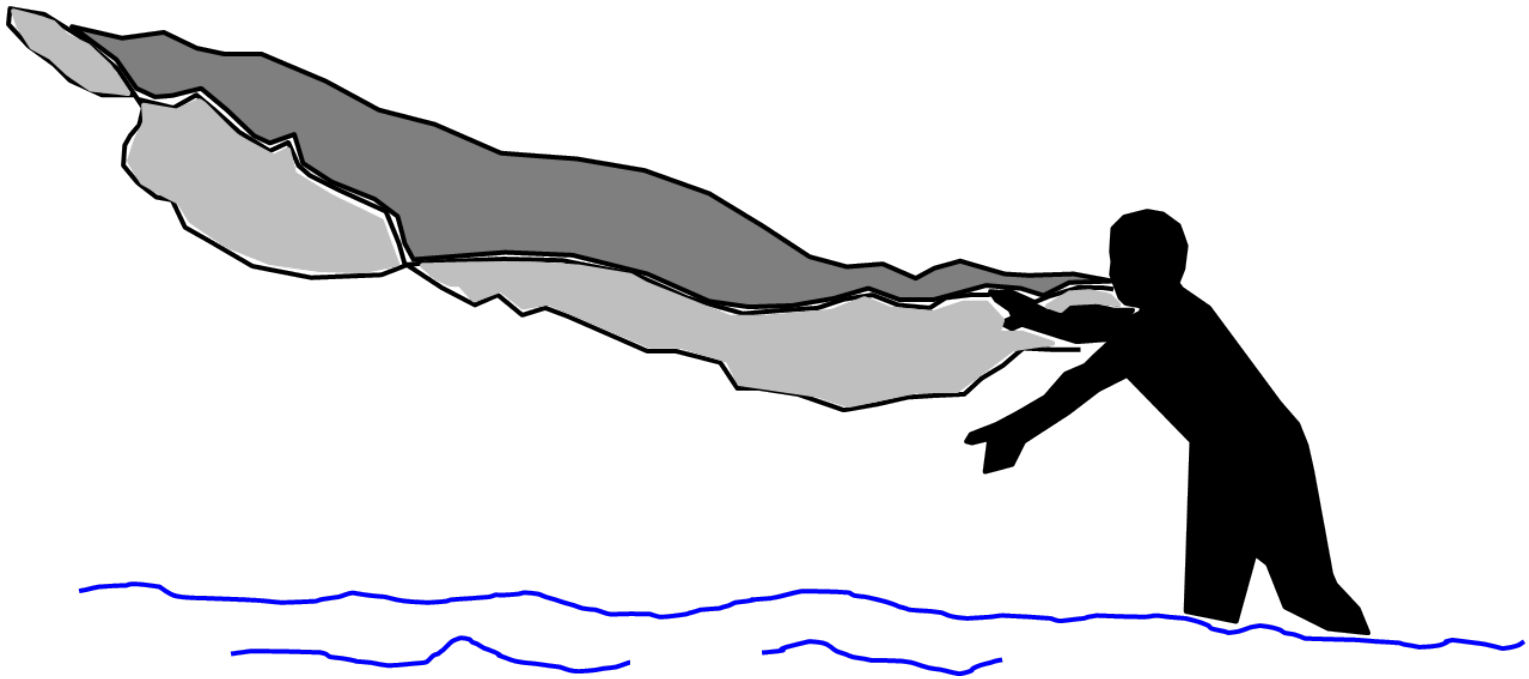
Or…. …

"What is …niquely hard or difficult?"

Risk ID methodologies: Independent assessments, Interviews with Integrated Product Team (IPT) leads, Review of similar/historical programs, Trade studies, Statement of Work (SOW) requirements, etc.

Risk Identification

Cast your net wide at first! Do not ignore areas or eliminate ideas early in the process.



All program personnel are encouraged to identify candidate risks.

Identifying Risk Ideas: Technical Risk Drivers

- Requirements
- Proprietary Data/Designs
- Technology
- Hardware State-of-the-Art
- Support Concepts
- Reliability and Maintenance
- Constraints
- Personnel
- Computer Resources
- Manufacturing Resources
- New Manufacturing/labs
- Standards
- Government Furnished Equipment/Personnel
- Environment
- Tools
- Data Rights
- Experience
- Documentation
- Management Approach

Software Specific Risks

- **Complexity**
- **Size**
- **Stability**
- **Developmental Approach**
- **Process Model**
- **Process Maturity**
- **Integration Approach**

Risk Identification Example

Good "If Then" Statements are Critical to effective Risk Management…

"There is a risk that if…" | Condition or Event | "then…" | Undesirable Consequence

Some negative event occurs

Pipes Freeze

Something bad may result

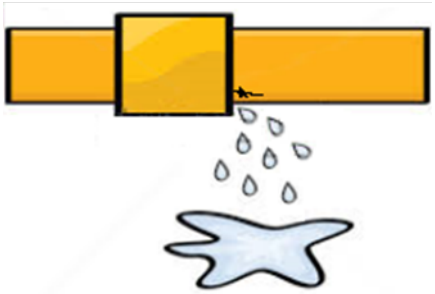
Water Damage

… but they are not enough. We must know WHY in order to do something about it (handling).

Root Cause Determination

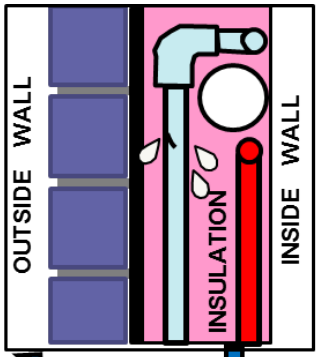
If

Pipes Freeze



Why?

Not Enough Insulation Between Pipe and Outside



Why?

Construction Not Built to Code

WHY?

Why?

Plumber Did not Follow Procedures

Why?

Unqualified General Contractor

Then

Water Damage

Ask “Why” multiple times until the root risk event(s) is (are) discovered

Lesson Plan Status

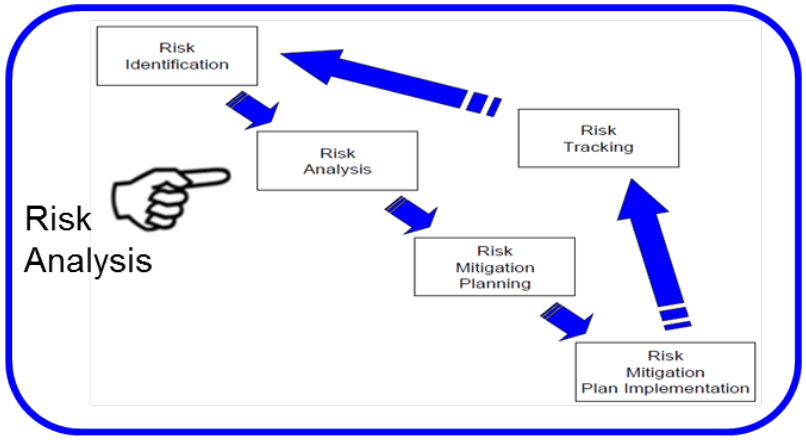
- Risk Overview
- Risk, Issue, and Opportunity Relationship
- IT Related Risks
- Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
- Lesson Review

Risk Statement—Exercise 1: JRATS/JTAMS Risks

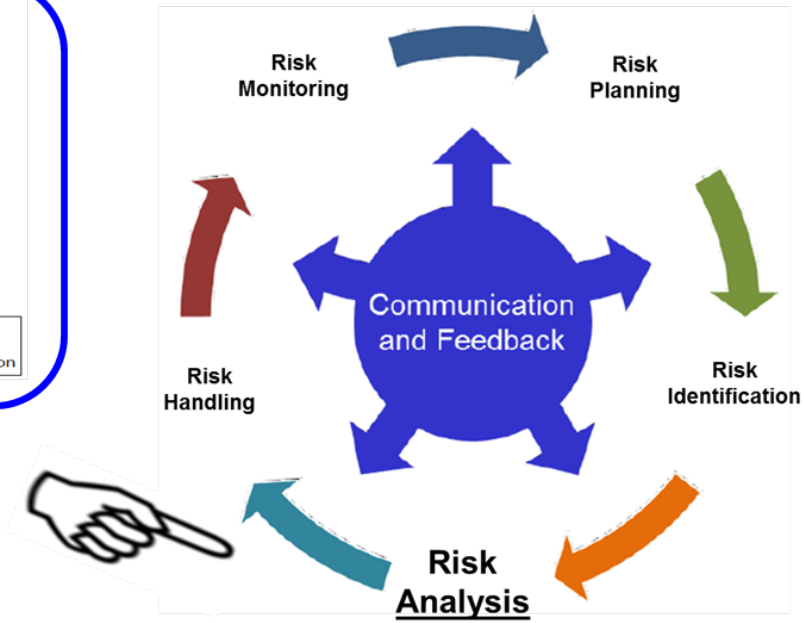
TASK: Write a proper Risk Statement for each of the following while you answer the question: “What could happen to us in Post Deployment Software Support (PDSS) Phase if things don’t change now?” Assume YOU are the PM stated in the situation.

- **Team 1**: PM JTAMS is re-using Army TAMS software. The TAMS OBD application has over 900 patches to it.
- **Team 2**: PM JTAMS is re-using Army TAMS software. All of the TAMS applications (OBD, PAMS and THS) come to us without documentation.
- **Team 3**: PM Firebird (FUAV) is using 50,000 SLOC of an old/obsolete programming language called TACPOL.
- **Team 4**: PM JTAMS is experiencing delays in the receipt of MRES software updates.
- **Team 5**: PM JCCS keeps changing their interfaces with FUAV, JUGV and JTAMS. As a result, PM JTAMS has no interface to design to.

Risk Analysis



DoD RMG v6 August, 2006

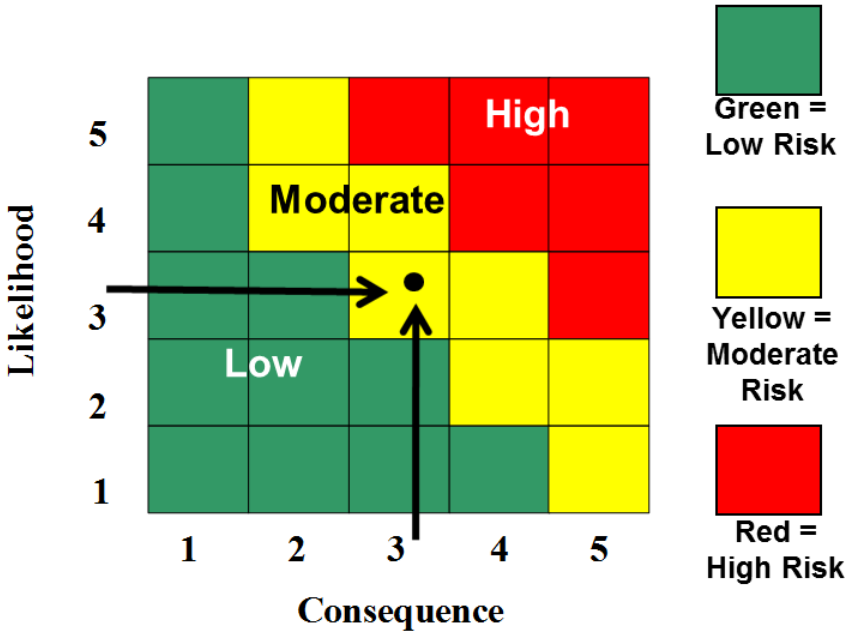


What is the likelihood and consequence of the risk? and …
How big is the risk?

- Evaluate the **impact** to the program (cost, schedule, and performance.)
- Assess **likelihood** of occurrence and the **consequences** in terms of technical, schedule, and cost (often color coded as red for high, yellow for moderate, and green for low risk.)
- The government and the contractor should seek to have a common framework for risk consequence and likelihood criteria.

How big is the risk and how likely is it to occur?

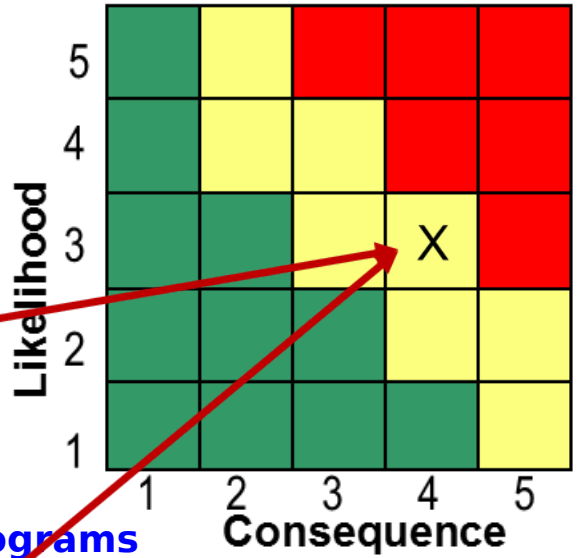
- Assess likelihood of occurrence
- Identify the possible consequences in terms of technical, schedule, and cost
- Assess consequence
- Identify the risk level in the 5X5 risk reporting matrix



Key Concept: Build the process **before** applying it!

Risk Analysis (Example)

Level	Likelihood	Probability of Occurrence
5	Near Certainty	> 80% to ≤ 99%
4	Highly Likely	> 60% to ≤ 80%
3	Likely	> 40% to ≤ 60%
2	Low Likelihood	> 20% to ≤ 40%
1	Not Likely	> 1% to ≤ 20%



Note: Underlined values must be tailored for specific programs or risks.

Level	Technical Performance	Schedule	Cost
1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact
2	Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program	Able to meet key dates. Slip < 1 month	Budget increase or unit production cost increase (< 1% of Budget)
3	Moderate reduction in technical performance or supportability with limited impact on program objectives	Minor schedule slip. Able to meet key milestones with no schedule float. Slip 1 to 2 month(s)	Budget increase or unit production cost increase (1 to 5% of Budget)
4	**Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success**	**Program critical path affected. Slip >2 to 4 months**	Budget increase or unit production cost increase (>5 to 10% of Budget)
5	Severe degradation in technical performance; Cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones. Slip > 4 months	Exceeds APB threshold (≥10% of Budget)

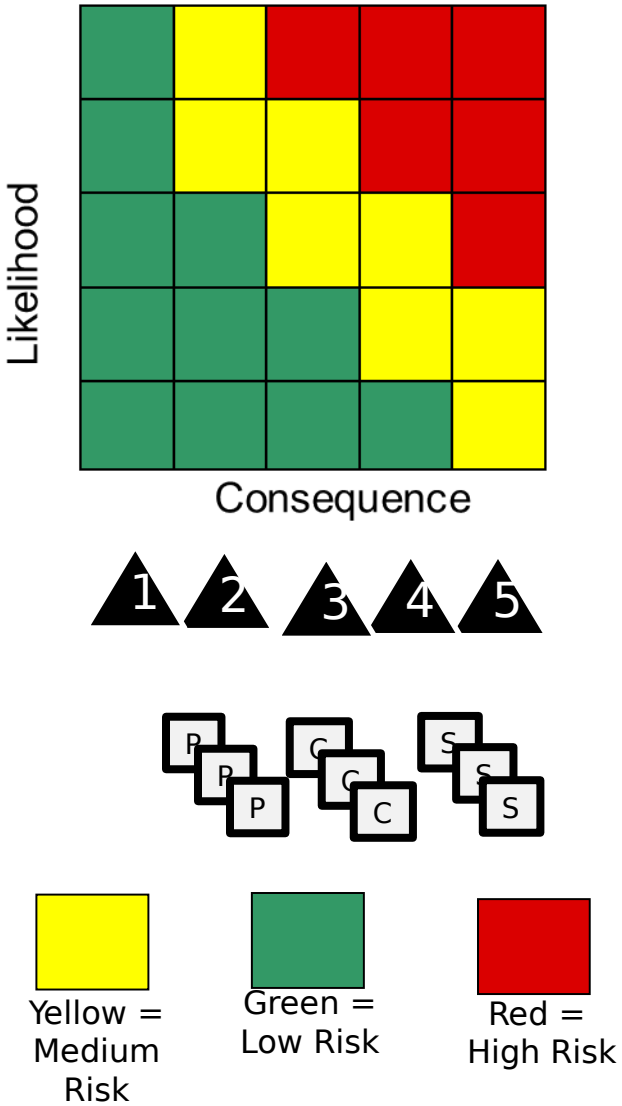
Lesson Plan Status

- Risk Overview
- Risk, Issue, and Opportunity Relationship
- IT Related Risks
- Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
- Lesson Review

Risk Analysis Exercise 2 JRATS Risk Analysis—Instructor Answers

TASK: Assess the likelihood and consequence of the risks identified earlier:

- **Team 1**: If PM JTAMS doesn't re-write the OBD application (re-factor it) and clean up the code design, it will be more costly and take more time to fix defects found or make modifications in the reused OBD software during PDSS.
- **Team 2**: If PM JTAMS doesn't take the time to understand and document the software design in the re-used TAMS applications, it will be more costly and take more time to fix defects found or make modifications during the PDSS phase.

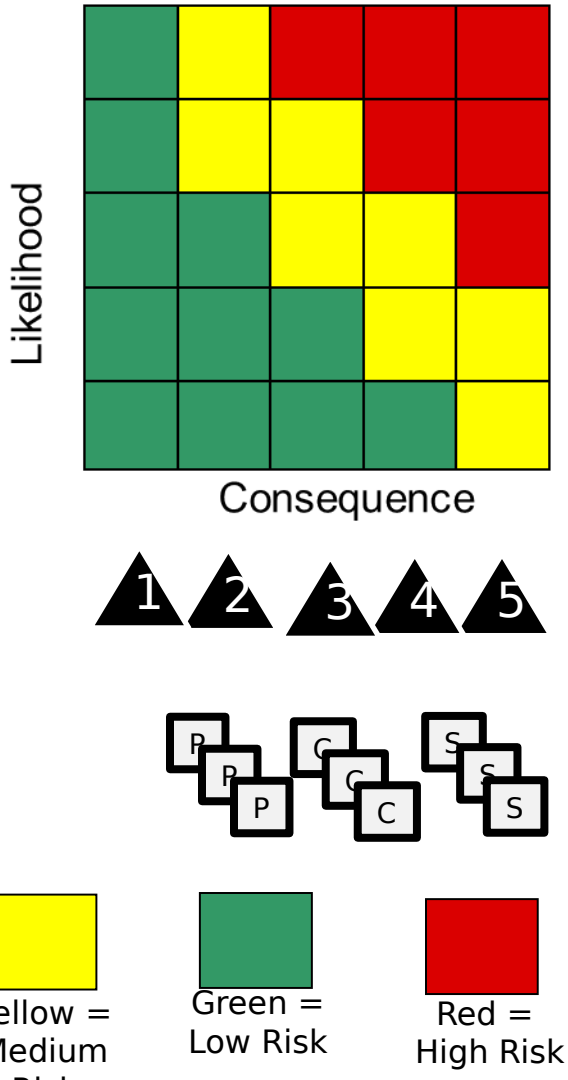


JRATS Risk Analysis (continued)

Risk Analysis Exercise 2 JRATS Risk Analysis—Instructor Answers

TASK: Assess the likelihood and consequence of the risks identified earlier:

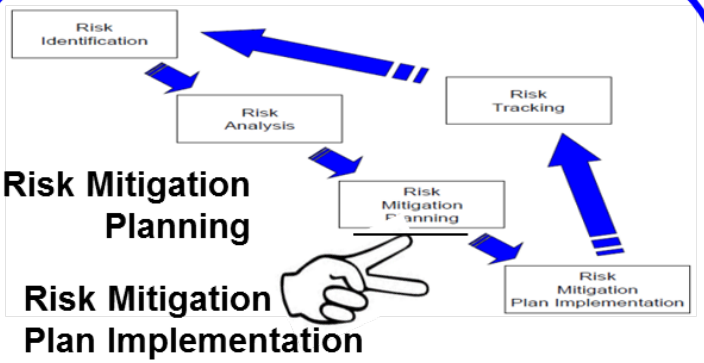
- **Team 3**: If PM FUAV doesn't re-write the 50,000 TACPOL SLOC, it will be more costly and take more time to fix defects found or make modifications during PDSS.
- **Team 4**: If the timeline established for JTAMS production is not met because of a delay in receiving MRES software updates, then there will be a program slip of at least 4 months.
- **Team 5**: If PM JCCS doesn't control their interface definitions, the JTAMS applications could stop working during PDSS.



Risk Analysis Expectations

- Risk statements and descriptions fully document events that could adversely affect a program's ability to meet cost, schedule, and performance objectives or baselines.
- Risk statements are clearly written using an "if–then" or similar construct.
- Programs use established criteria, tailored only as necessary, to provide a consistent means for evaluating risks.
- Resulting likelihood and consequence ratings should be supported by data and analysis.
- Programs conduct periodic risk analyses to update risk estimates and to align with other program activities such as Earned Value Management (EVM), Integrated Master Schedule (IMS), and technical reviews.
- If the analyzed likelihood is 100 percent, the program should address the event or condition as an issue rather than a risk.
- Risks are characterized as low, moderate, or high based on placement of the likelihood and the maximum of the three consequence values on the risk matrix.

Risk Handling



DoD RMG v6 August, 2006

DoD RIOG Jun '15

Risk Handling

- Consider the accept, avoid, and transfer handling options, not just the mitigation option.
- Choose the best handling option, then select the best implementation approach for that option.
- Take into consideration elevating the risk to appropriate tiers (executive, management, or working level.)
- The selected handling strategy for program-level risks should be reflected in the program's Acquisition Strategy and presented at all relevant decision points and milestones.

- It should include the specifics of what should be done; when it should be accomplished; who is responsible; cost, schedule, and performance impacts; and the resources required to implement the risk handling plan.

Acceptance, Avoidance, and Transfer

- **Risk Acceptance**: The program acknowledges that the risk event or condition may be realized.
  - Accepting a risk does not mean it should be ignored.
  - Before accepting the risk, the program should identify the resources and schedule that would be needed should the risk be realized.
- **Risk Avoidance**: The program reduces or eliminates the risk event or condition by taking an alternate path.
  - Eliminate the source of the risk and replace it with a lower risk solution.
  - This option should be used only if the selected implementation approach truly results in the desired effect and reduced risk likelihood and/or consequence.
- **Risk Transfer**: Reassigning the risk responsibility to another entity.
  - Transference of risk does not eliminate all responsibility and risks must be monitored for potential consequences.
  - The transfer option may be viable only if it results in an acceptable risk likelihood and/or consequence posture.

Risk Mitigation (formally Control)

- **Risk Mitigation** seeks to **actively** reduce risk to an acceptable level. Mitigation generally entails **taking action** to reduce the likelihood, and on occasion the consequence, of a risk to as low as possible in order to **minimize potential program impacts**.

- Risk mitigation plan implementation reduces level of program risks by:
  - **Directing** the teams to execute the defined and approved risk control plans
  - **Applying resources** (manpower, schedule, budget) to reduce the likelihood and/or consequence of risks
  - **Tracking** resource expenditure, technical progress, and risk impacts (benefits)
  - Outlining the risk reporting requirements for ongoing monitoring, to include “trip wires” which warrant elevating the risk to the next management level

Risk Mitigation Approaches

- Multiple Development Efforts: Create competing systems in parallel that meet the same performance requirements.
- Early Prototyping: Build and test prototypes early in the system development.
- Incremental Development: Defer capability to a follow-on increment.
- Technology Maturation: Use when a desired technology will replace an existing technology.
- Design of Experiments: Identify critical design factors that are sensitive, therefore potentially high risk, to achieve a particular user requirement.
- Open Systems, Standard Items, or Software Reuse: Select commercial specifications and standards or use. existing and proven hardware and software, where applicable.
- Models and Simulation: Investigate various design options and system requirement levels.

Risk Mitigation Plan

1. Identify and lay out the risk handling activities in a sequential manner, using realistic and logical schedule precedence
2. Ensure all risk handling activities:
   a) are clearly defined and jargon free,
   b) are objective and not subjective, and
   c) have specific, measurable outcomes.

	Action	Who	What	When
1				
2				
3				
4				

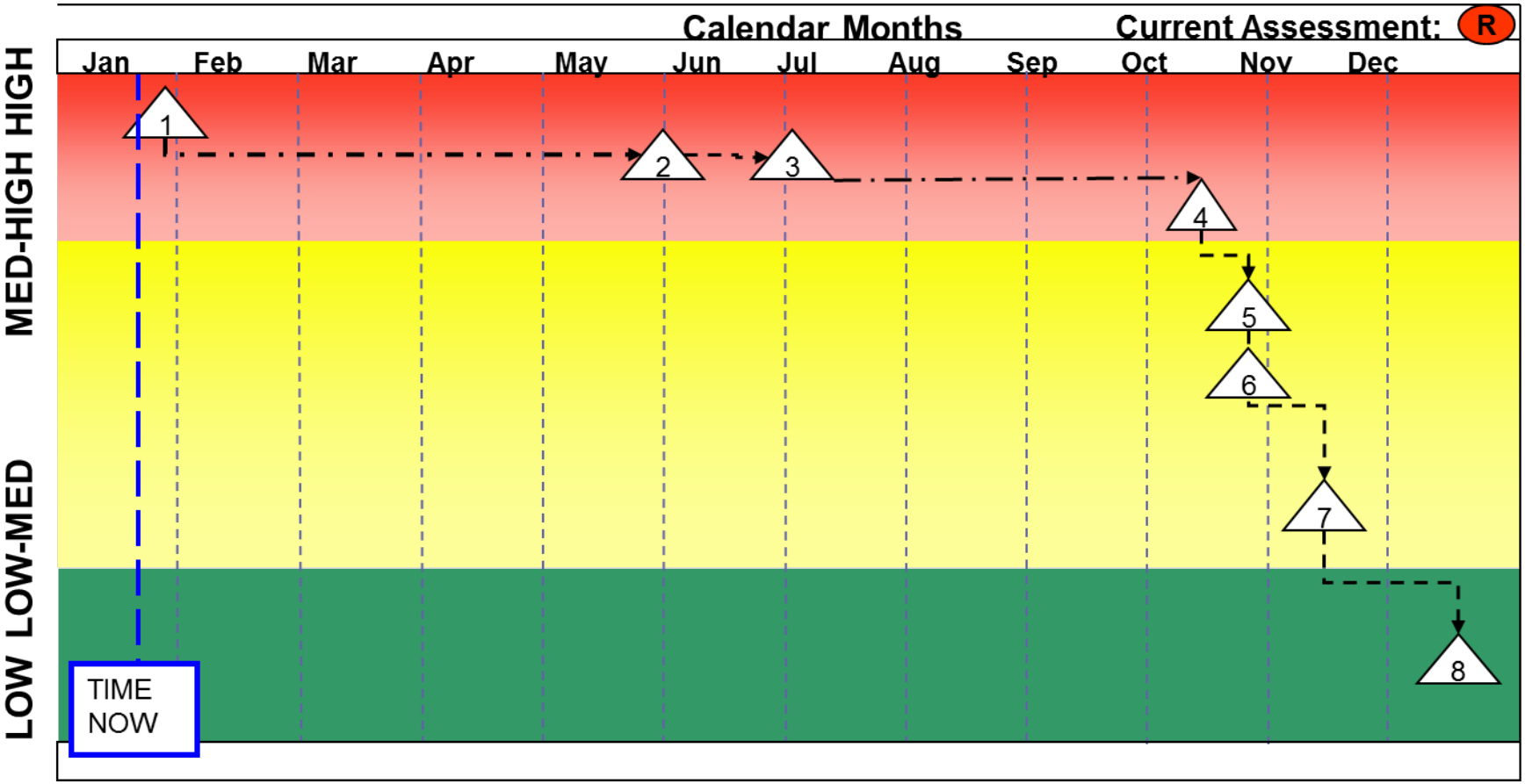
Example: Is the statement "performing a test" an appropriate activity?

How about? "brassboard throughput test results met or exceeded all performance thresholds requirements, and the results are approved by the user"

3. Assign a planned likelihood and consequence value to each risk handling activity
4. Estimate the start and finish dates for each risk handling activity.
5. Include the risk handling activities or a subset of these activities in the program IMS.
6. Chart the relationship of risk handling activities, plotting risk level versus time to estimate their relative risk burn-down/reduction

Risk Burn-Down Chart

- An instant snapshot of the progress of a risk over time
- Actual progress against the planned reduction of risk levels



Lesson Plan Status

- Risk Overview
- Risk, Issue, and Opportunity Relationship
- IT Related Risks
- Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
- Lesson Review

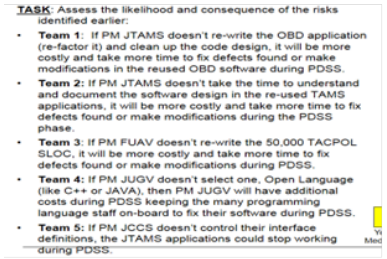
Risk Handling—Exercise 3

Step 1: Start with your initial scenario and the Risk matrix you developed

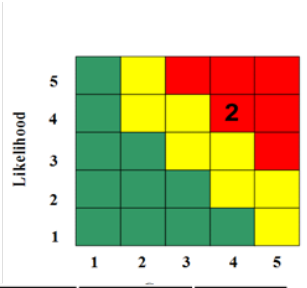
Step 2: Identify **detailed steps** that will drive risk to an acceptable level given program constraints and objectives

Step 3: Develop the “Waterfall Chart”

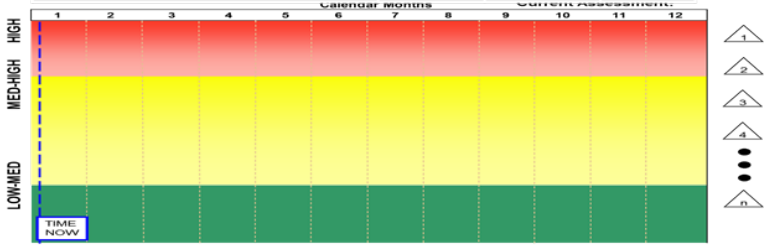
Step 4: Adjust Risk Matrix Expectation consistent with Mitigation Planning

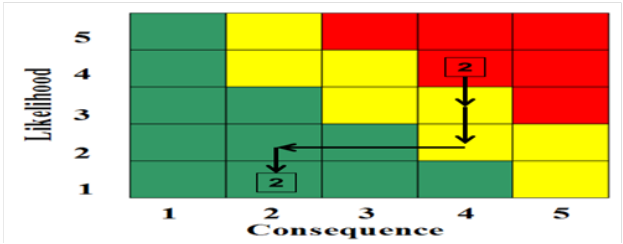

TASK: Assess the likelihood and consequence of the risks identified earlier:

- **Team 1**: If PM JTAMS doesn't re-write the OBD application (re-factor it) and clean up the code design, it will be more costly and take more time to fix defects found or make modifications in the reused OBD software during PDSS.
- **Team 2:** If PM JTAMS doesn't take the time to understand and document the software design in the re-used TAMS applications, it will be more costly and take more time to fix defects found or make modifications during the PDSS phase.
- **Team 3**: If PM FUAV doesn't re-write the 50,000 TACPOL SLOC, it will be more costly and take more time to fix defects found or make modifications during PDSS.
- **Team 4:** If PM JUGV doesn't select one, Open Language (like C++ or JAVA), then PM JUGV will have additional costs during PDSS keeping the many programming language staff on-board to fix their software during PDSS.
- **Team 5:** If PM JCCS doesn't control their interface definitions, the JTAMS applications could stop working during PDSS.



Action	Who	What	When
1			
2			
3			
4			



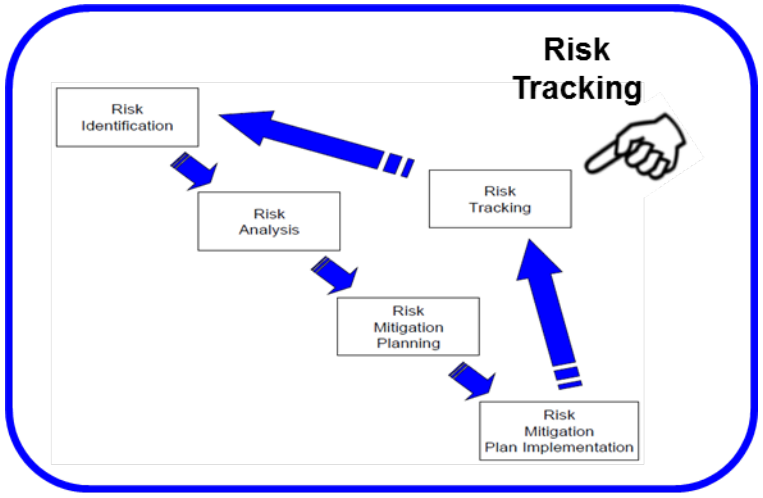


SEE EXERCISE FOLDER ON STUDENT CD (LSN 10) FOR TEMPLATES

Risk Handling Expectations

- Risks can be accepted, avoided, transferred, or mitigated.
- Risk mitigation activities typically reduce the likelihood of the risk event occurring.
- Risks are managed at the appropriate organizational level (executive, management, or working). The program tracks the development and implementation of the risk handling plan.
- The program allocates appropriate budget and other resources to implement the handling plan and enters mitigation activities into the IMS.
- Risks that are assessed as high have resourced risk handling plans. Moderate risks should also typically have resourced risk handling plans, as appropriate.
- Risk burn-down plans should be time-phased and include specific measurable handling activities; meetings do not burn down risks.

Risk Monitoring (formerly Tracking)



DoD RMG v6.0 August, 2006

Risk monitoring includes recording, maintaining, and reporting of risks, risk analyses, risk handling, and tracking results.

Answers the question: "How are things going?"

Risk Monitoring

When Monitoring Risks

- Track the implementation and progress of the risk handling
- TPMs are an integral risk monitoring activity
- Conduct regular status updates to monitor risks for changes to likelihood and/or consequences
- Document active risks as well as those that can be retired - prevent unnoticed relapse of retired risks

Expectations

- The program team conducts regular status updates
- PMOs and contractors establish a regular schedule for reviewing risks.
- Team alerts management when risk handling plans should be adjusted.
- Program team tracks actual versus planned implementation of progress against the risk handling plan.
- Program reviews closed risks periodically to ensure their risk level has not changed.

Alert the next level of management when the ability to handle a risk exceeds the lower level's authority or resources.

Lesson Plan Status

- Risk Overview
- Risk, Issue, and Opportunity Relationship
- IT Related Risks
- Risk Management Process
  - Exercise 1
  - Exercise 2
  - Exercise 3
- Lesson Review

Lesson Review

- Risk Overview
- Risk, Issue, and Opportunity Relationship
- IT Related Risk
- Risk Management Process

DoD Risk, Issue, and Opportunity Management Guide June 2015

Summary

Today we learned to:

- Define the elements that constitute an effective Risk Management (RM) program for an IT system acquisition.
- Identify the two components of risk.
- Identify how risk , issue, and opportunity management interrelate.
- Identify risks inherent to Information Technology (IT) system acquisition.
- Apply the five components of the DOD Risk Management Process Model to a given IT acquisition scenario.